FIG. 1

Internet

Wireless portable Internet

40

AAA server

30

31

20

21

BS

SS

10
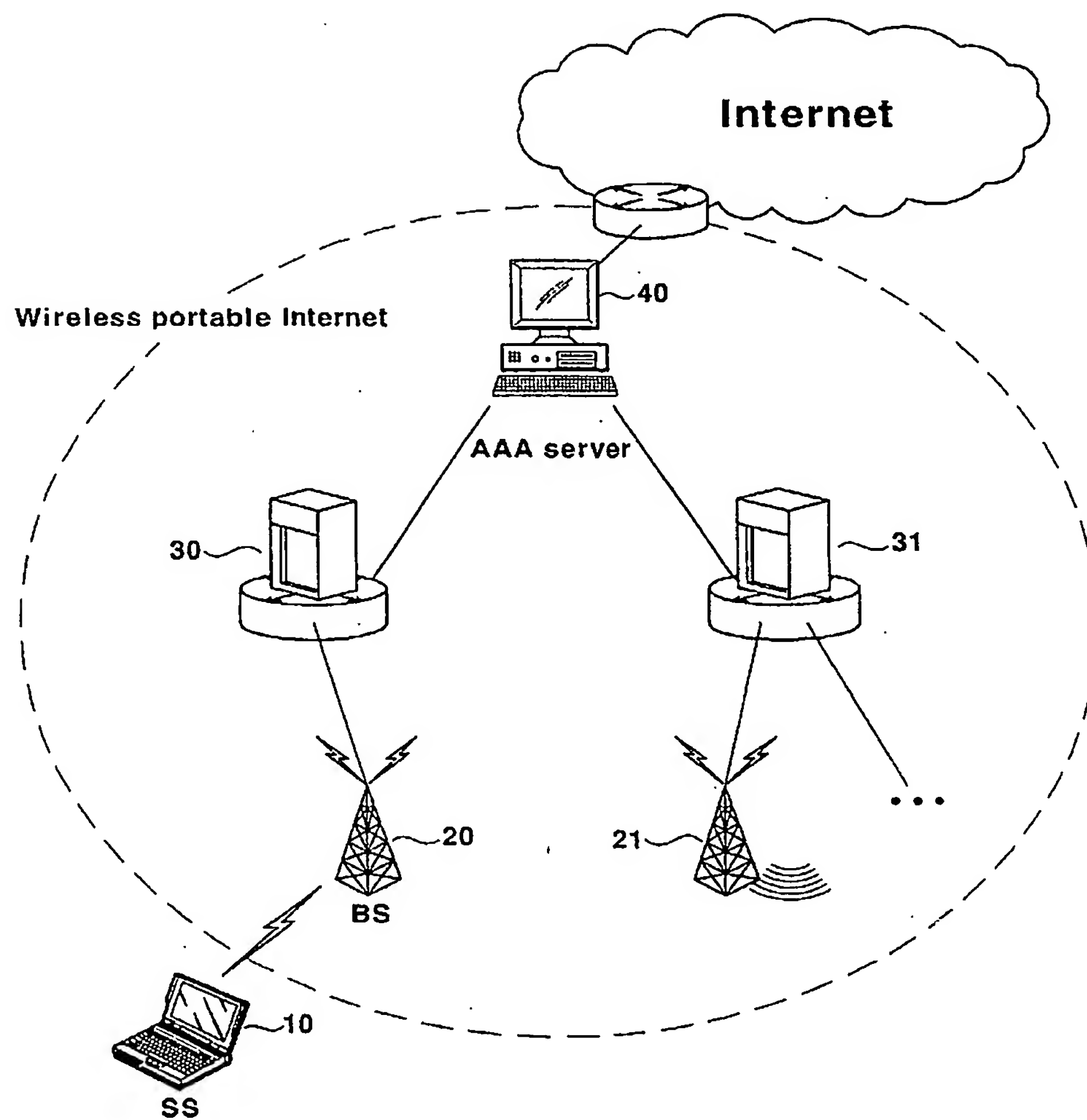
FIG. 2

FIG. 3

FIG. 4

```
        ( Enter BS )──S10
              │
              ▼
   ┌──────────────────────────┐
   │ Establish downlink sync  │
   │ and acquire uplink parameter │──S20
   └──────────────────────────┘
              │
              ▼
   ┌──────────────────────────┐
   │          Range           │──S30
   └──────────────────────────┘
              │
              ▼
   ┌──────────────────────────┐
   │ Negotiate SS basic capabilities │──S40
   └──────────────────────────┘
              │
              ▼
   ┌──────────────────────────┐
   │      Authenticate SS     │──S50
   └──────────────────────────┘
              │
              ▼
   ┌──────────────────────────┐
   │ Generate and distribute TEK │──S60
   └──────────────────────────┘
              │
              ▼
   ┌──────────────────────────┐
   │        Register SS       │──S70
   └──────────────────────────┘
              │
              ▼
   ┌──────────────────────────┐
   │  Establish IP connection │──S80
   └──────────────────────────┘
              │
              ▼
   ( Establish traffic connection )──S90
```

FIG. 5

SS
(10)

BS
(20)

Key Request (Prim.Management CID)

{SA-ID # : n}

S100

Key Reply (Prim.Management CID : TEK$_x$)

{SA : n}

S110

TEK$_x$
Active
Lifetime

S120

S140

TEK Refresh
Timeout

S130

TEK
Grace
Time

Key Request (Prim.Management CID)

{SA-ID # : n}

S150

Key Reply (Prim.Management CID : TEK$_{x+1}$)
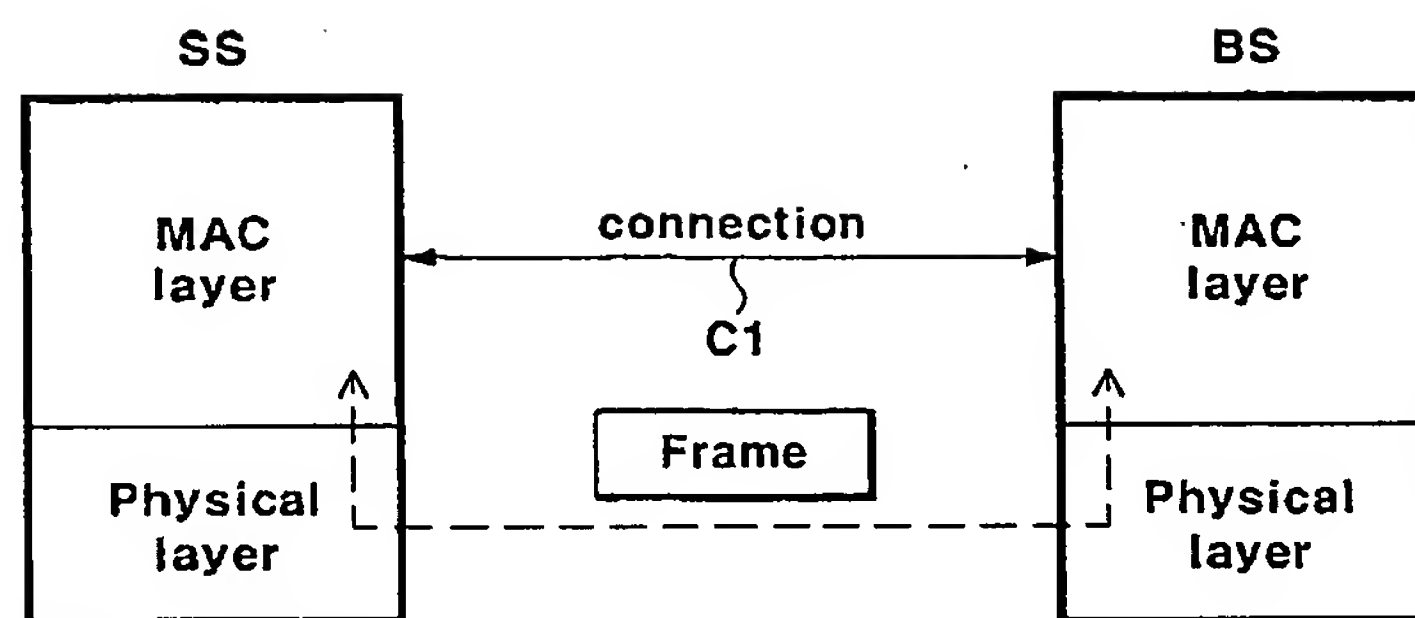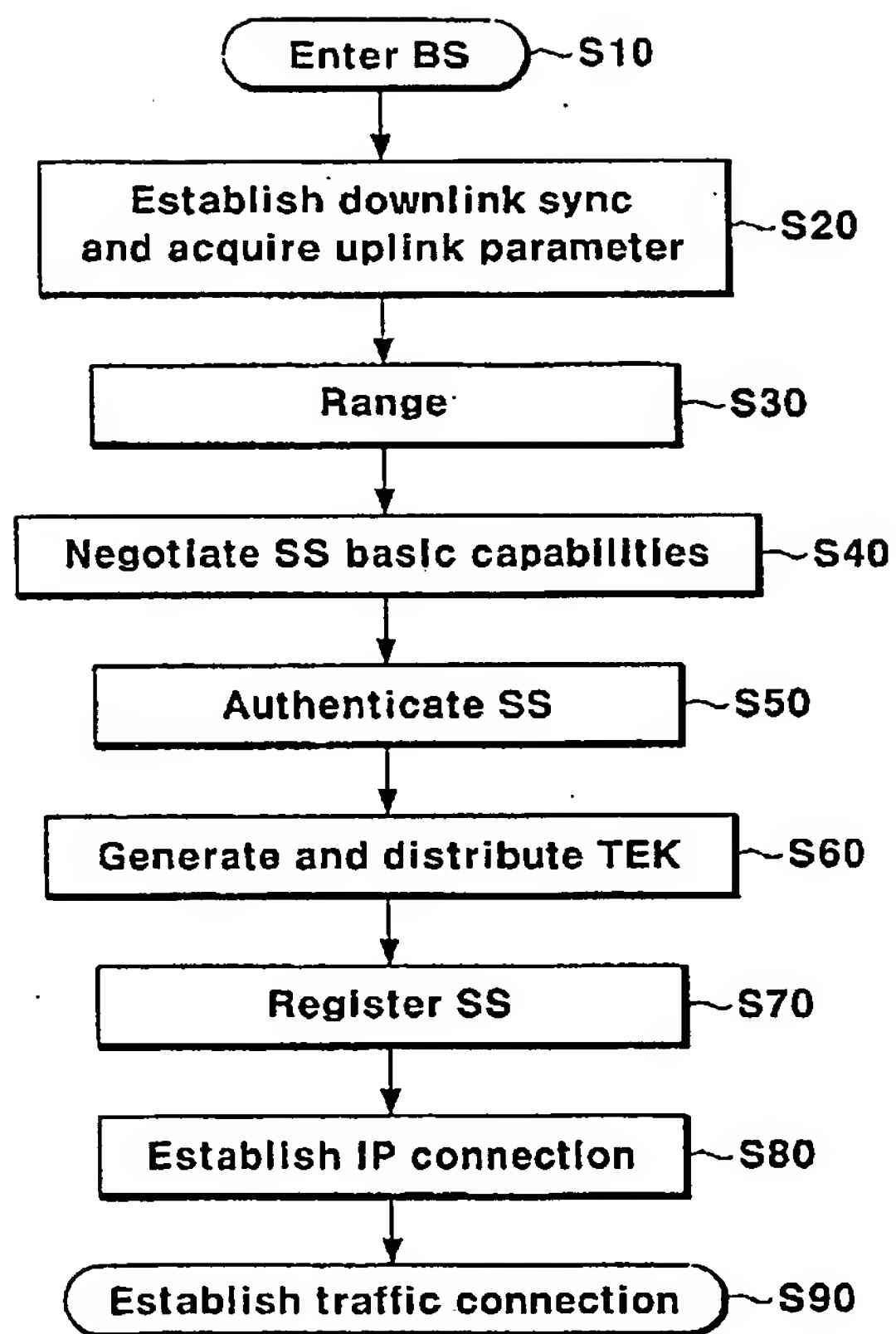
{SA # : n}

S160

S170

TEK$_{x+1}$
Active
Lifetime

FIG. 6

FIG. 7

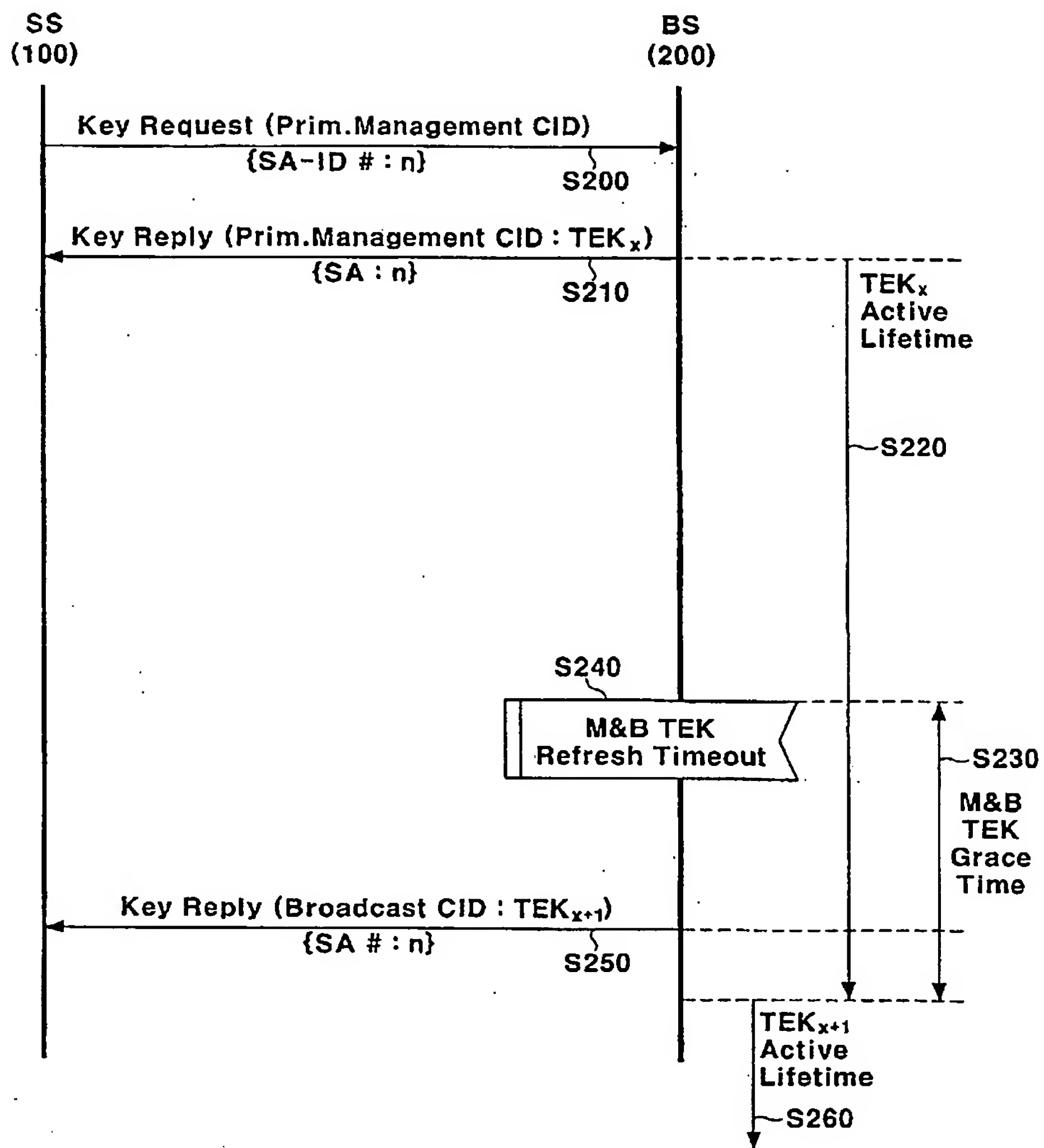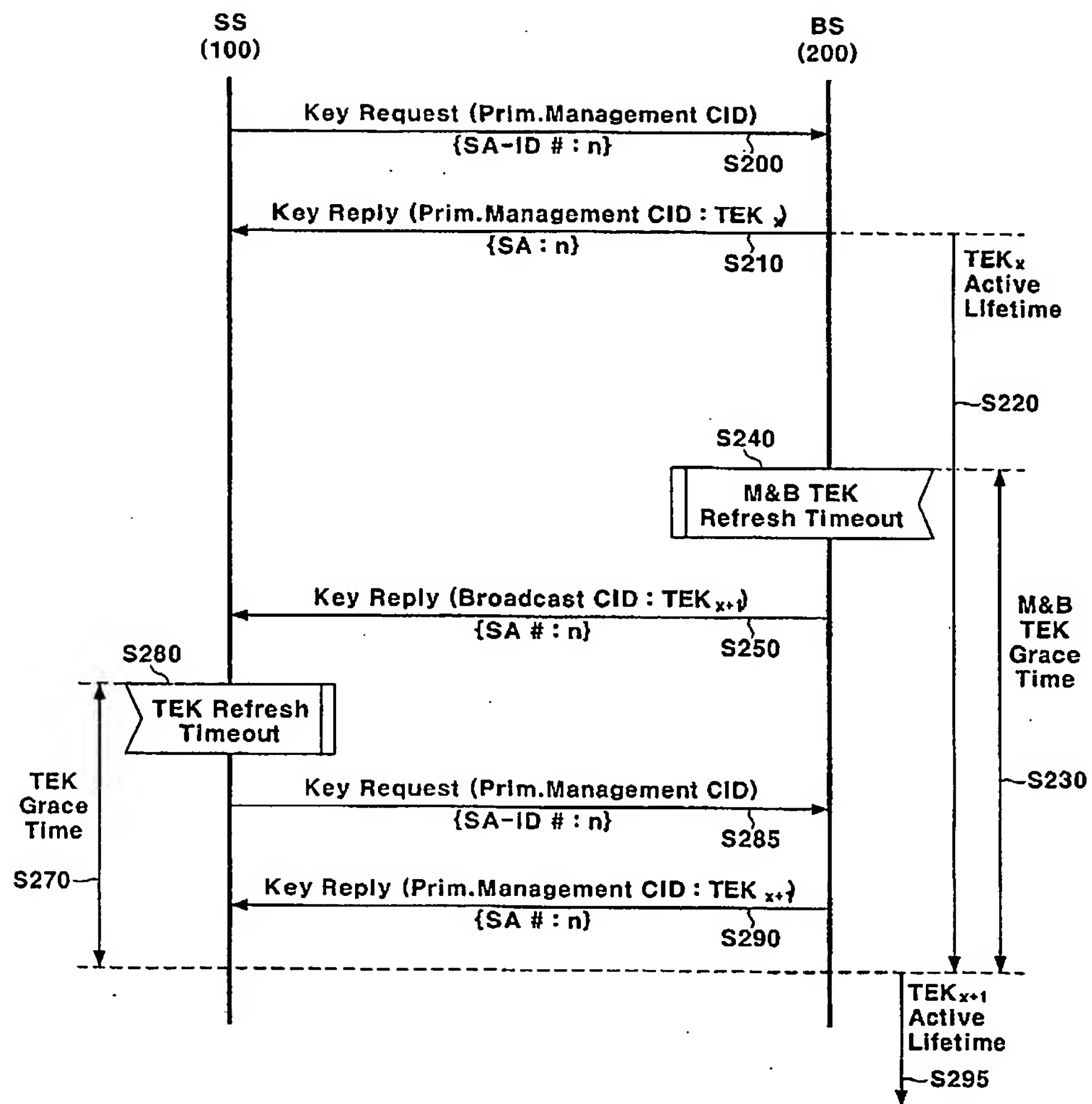| System	Name	Description	Minimum value	Default value	Maximum value
BS	M&B TEK Grace Time	Time prior to TEK (for the multicast and broadcast traffic service) expiration BS begins rekeying. This time is longer than the TEK Grace Time.	Vendor-specific value	Vendor-specific value	Vendor-specific value

FIG. 8

SS
(100)

BS
(200)

Key Request (Prim.Management CID)

{SA-ID # : n}   S200

Key Reply (Prim.Management CID : TEK$_x$)

{SA : n}   S210

TEK$_x$
Active
Lifetime

~S220

S240

┌────────────────────┐
│   M&B TEK   │
│ Refresh Timeout   │
└────────────────────┘

~S230

M&B
TEK
Grace
Time

Key Reply (Broadcast CID : TEK$_{x+1}$)

{SA # : n}   S250

TEK$_{x+1}$
Active
Lifetime

~S260

FIG. 9

FIG. 10
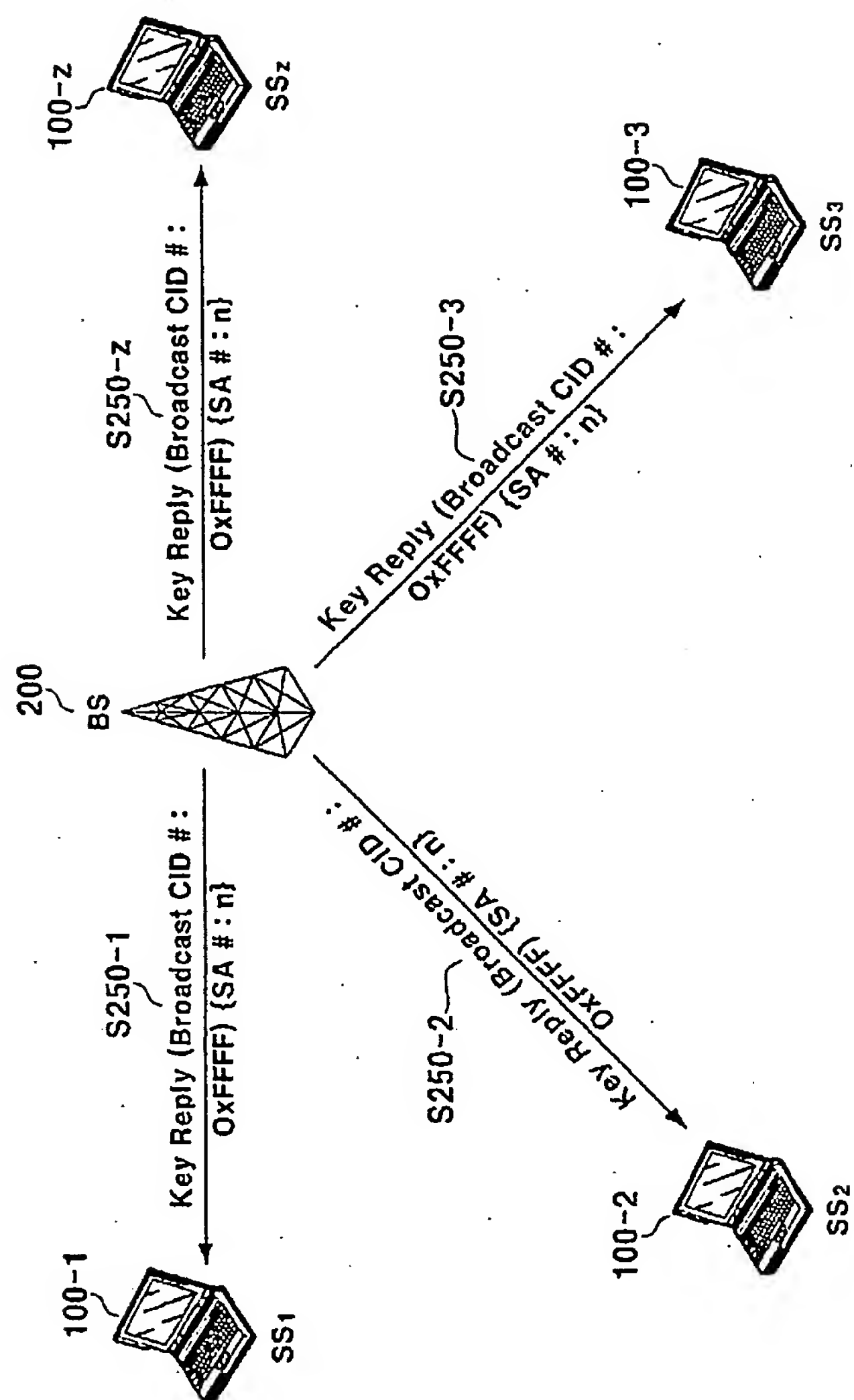
FIG. 11

CID(MAC Header)	Key to encrypt the TEK
Primary Management CID	KEK(Derived from the AK)
Broadcast CID	Old distributed TEK

FIG. 12

```
                    SS                                    BS
                   (100)                                 (200)
                     │                                     │
                     │    Key Request (Prim.Management CID)│
                     │────────────────────────────────────▶│
                     │         {SA-ID # : n}      S300     │
                     │                                     │
                     │     Key Reply (Prim.Management CID : TEK)    ┌ ─ ─ ─ ─ ─ ─
                     │◀────────────────────────────────────│       │ TEKx
                     │            {SA : n}        S310     │       │ Active
                     │                                     │       │ Lifetime
                     │                                     │       │
                     │                                     │       │
                     │                                     │       │─ S320
                     │                                     │       │
                     │                                     │       │
                     │                                     │       │
                     │                                     │       │
                     │   Key Update Command (GKEK update mode)      │
                     │◀────────────────────────────────────│       │
                     │ S330      (Prim. Management CID)     │       │
                     │                                S350 │       │
                     │                                     │  ┌ ─ ─ ─ ─ ─
                     │                            ┌────────┤  │
                     │                            │ M&B TEK│  │─ S340
                     │                            │Refresh Timeout   │ M&B
                     │   Key Update Command (TEK update mode)    │ TEK
                     │◀────────────────────────────────────│  │ Grace
                     │           (Broadcast CID)   S360    │  │ Time
            ┌ ─ ─ ─ ─│                                     │  │
            │ TEKx   │                                     │  │
            │ Grace  │                                     │  │
            │ Time   │                                     │  │
            └ ─ ─ ─ ─│                                     └ ─│─ ─ ─
                     │                                     │ TEKx+1
                     │                                     │ Active
                     │                                     │ Lifetime
                     │                                     │─ S370
                     │                                     ▼
```
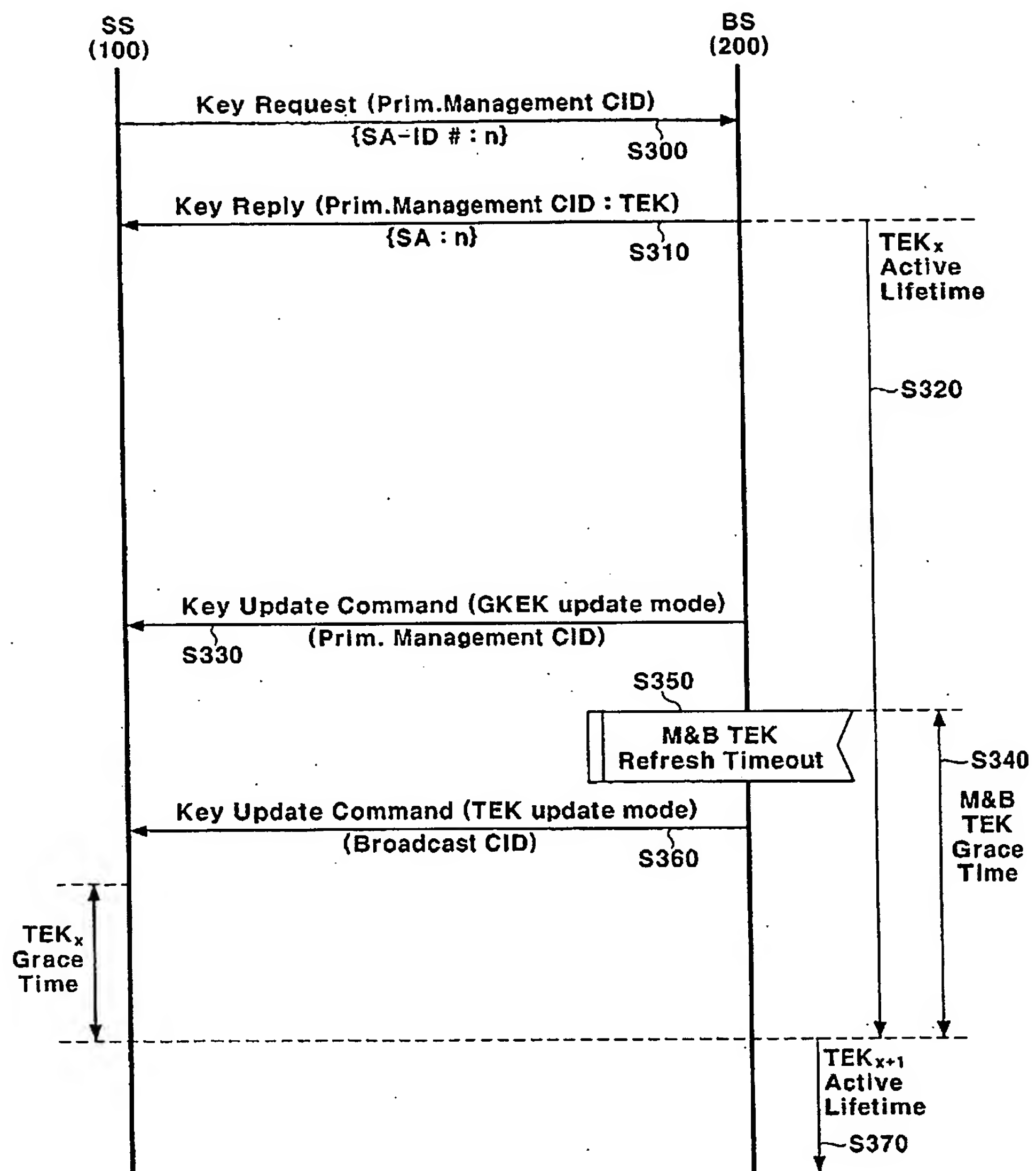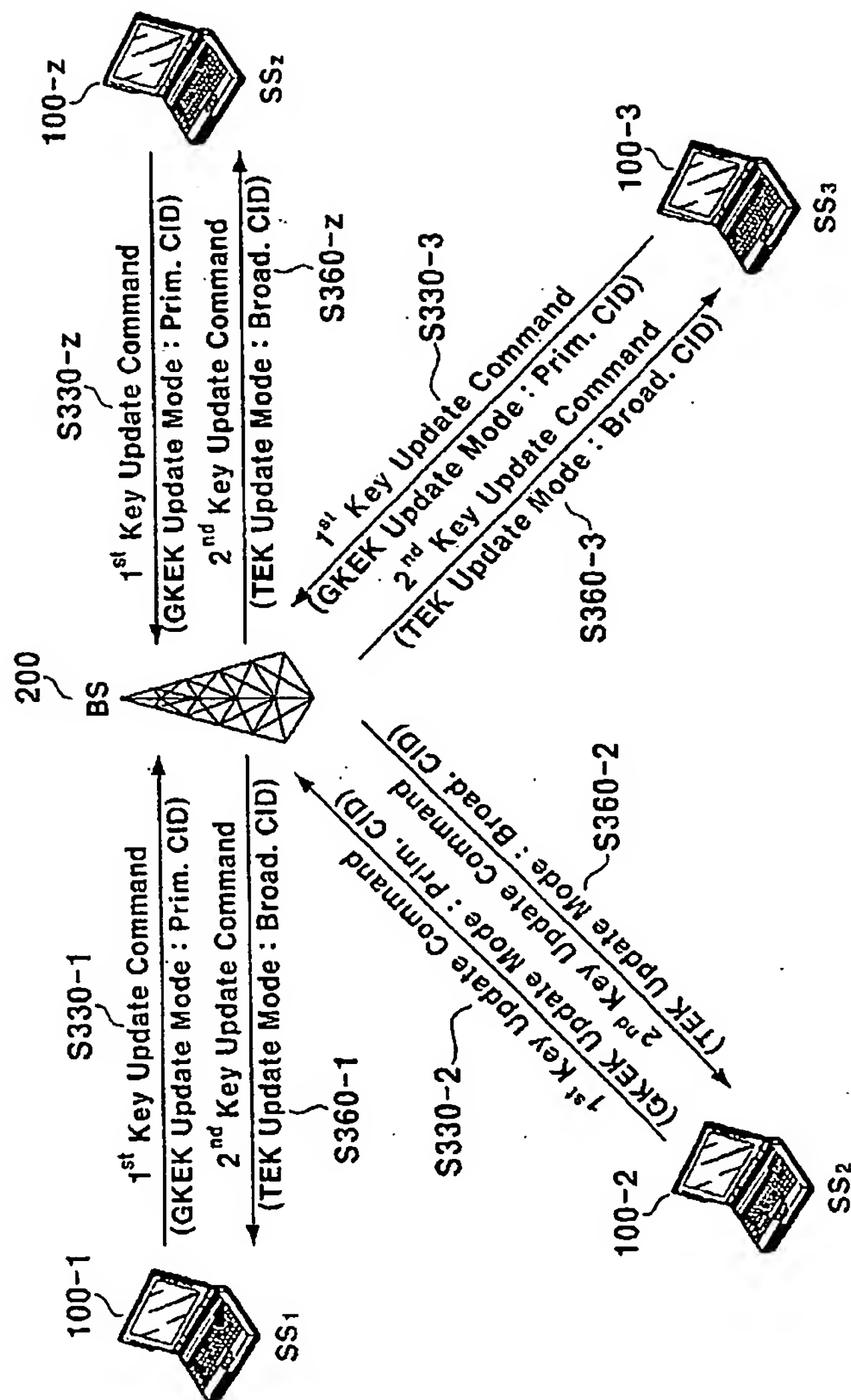
FIG. 13

FIG. 14

Attributes	Contents
Key-Sequece-Number	Authorization Key sequence number
SAID	Security Association ID
TEK-Parameters	"Older" generation of key parameters relevant to SAID
TEK-Parameters	"Newer" generation of key parameters relevant to SAID
HMAC-Digest	Keyed SHA message digest

FIG. 15

Attributes	Contents
GKEK	GKEK, encrypted with the AK
TEK	TEK, encrypted wity the GKEK (Multicast or Broadcast Service) or encrypted with the KEK (Unicast Service)
Key-Lifetime	TEK Remaining Lifetime
Key-Sequence-Number	TEK Sequence Number
CBC-IV	Cipher Block Chaining (CBC) Initialization Vector

FIG. 16

Attributes	Contents	1st Message (Primary)	2nd Message (Braodcast)
Key-Sequence-Number	Authorization key sequence number	O	O
SAID	Security Association ID	O	O
Key Push Modes	Usage code of Key Update Command message	O	O
Key Push Counter	Counter one greater than that of older generation for reply attack	O	O
TEK-Parameters	"Newer" generation of key parameters relevant to SAID		
> GKEK	GKEK, encrypted with the AK	O	×
> TEK	TEK, encrypted with the GKEK(Multicast or Broadcast Service)	×	O
> Key-Lifetime	TEK Remaining Lifetime	×	O
> Key-Sequence-Number	TEK Sequnce Number	O	O
> CBS-IV	Cipher Block Chaining (CBC) Initialization Vector	×	O
HMAC-Digest	Keyed SHA message digest	O	O

FIG. 17

Type	Length	Value
30	1	0, GKEK update mode (1st Message) 1, TEK update mode (2nd Message) 2-225, reserved

FIG. 18

Key push modes	Input Key
GKEK update mode	AK
TEK update mode	GKEK

FIG. 19
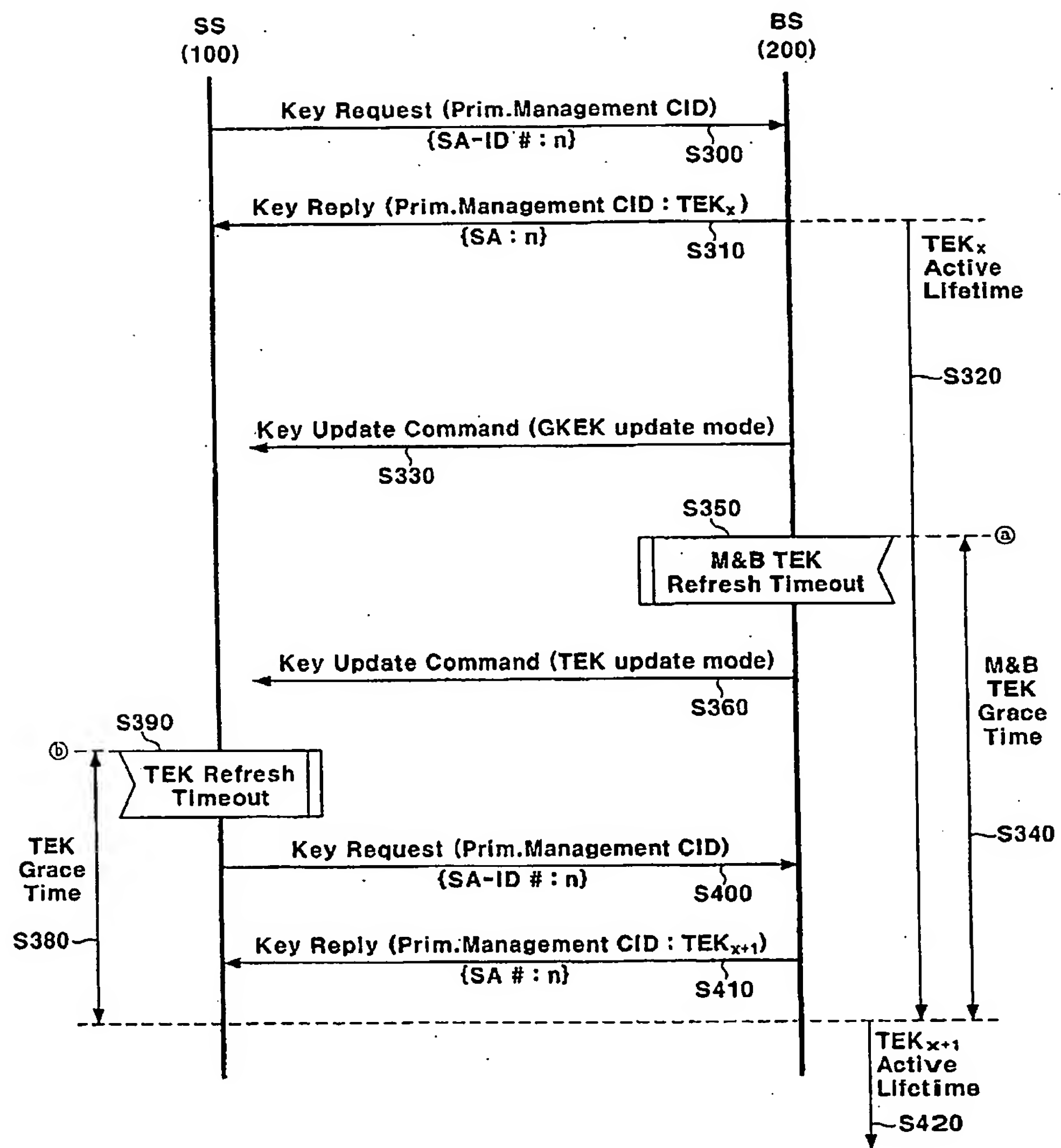
SS   BS
(100)   (200)

Key Request (Prim.Management CID)
{SA-ID # : n}   S300

Key Reply (Prim.Management CID : TEK$_x$)
{SA : n}   S310

                                                       TEK$_x$
                                                       Active
                                                       Lifetime

                                                       ⌐S320

Key Update Command (GKEK update mode)
        S330

                                    S350

                        ┌─────────────────┐
                        │   M&B TEK   │   ─ⓐ
                        │ Refresh Timeout │
                        └─────────────────┘

Key Update Command (TEK update mode)
                                S360   M&B
                                                       TEK
                                                       Grace
        S390   Time
ⓑ┐   ┌──────────────┐
     │ TEK Refresh   │
     │   Timeout   │
     └──────────────┘
TEK   Key Request (Prim.Management CID)   ⌐S340
Grace   {SA-ID # : n}   S400
Time
S380┐   Key Reply (Prim.Management CID : TEK$_{x+1}$)
               {SA # : n}   S410

                                                       TEK$_{x+1}$
                                                       Active
                                                       Lifetime

                                                       ⌐S420

FIG. 20

Situation	Transferred TEK-parameter information
Initial TEK response (before ⓐ)	TEK-parameters$_c$
Initial TEK response (after ⓐ)	TEK-parameters$_c$ & TEK-parameters$_N$
Initial update response (after ⓑ)	TEK-parameters$_N$

C : Current generation of key parameters relevant to SAID
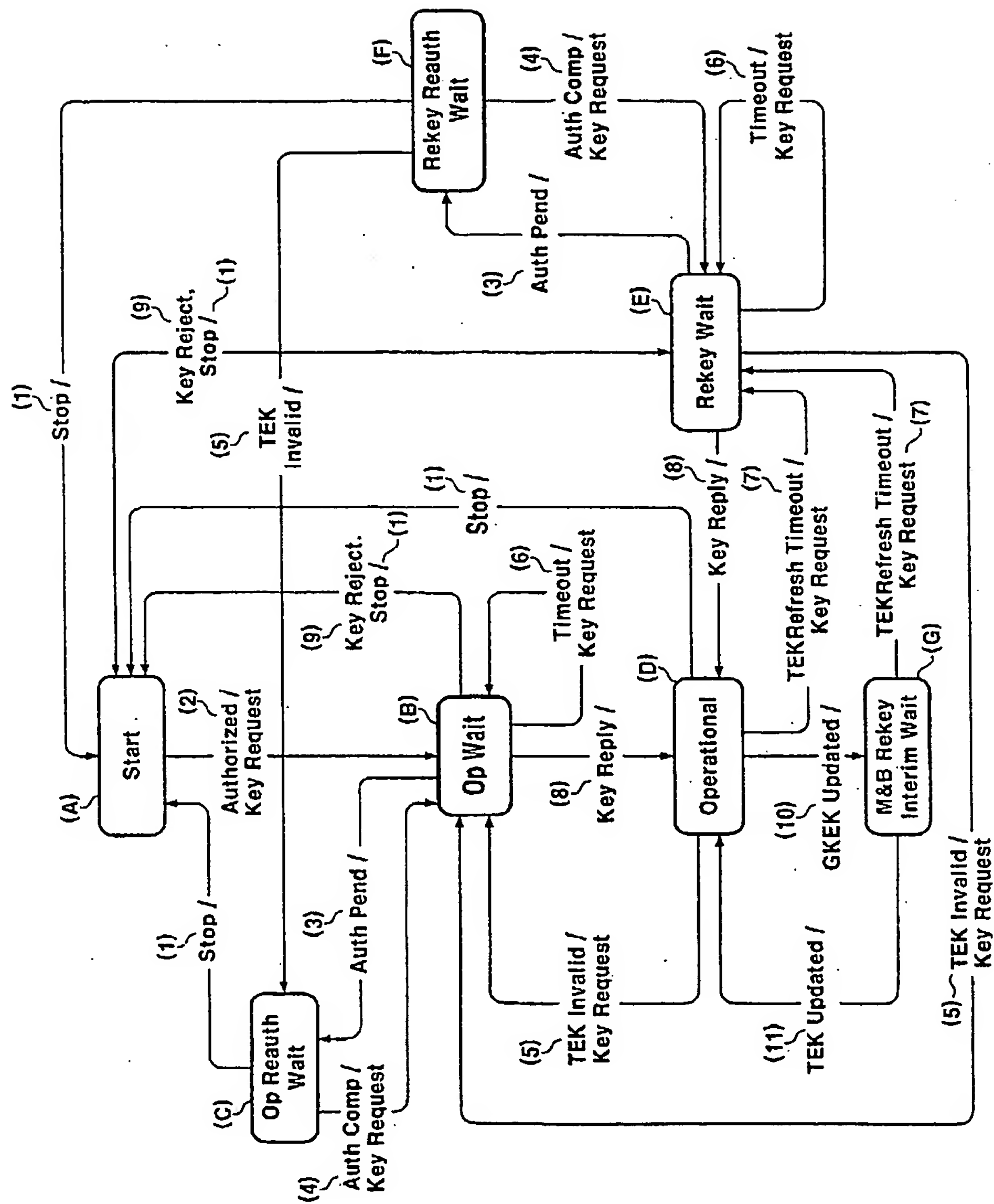
N : Next generation of key parameters relevant to SAID

FIG. 21
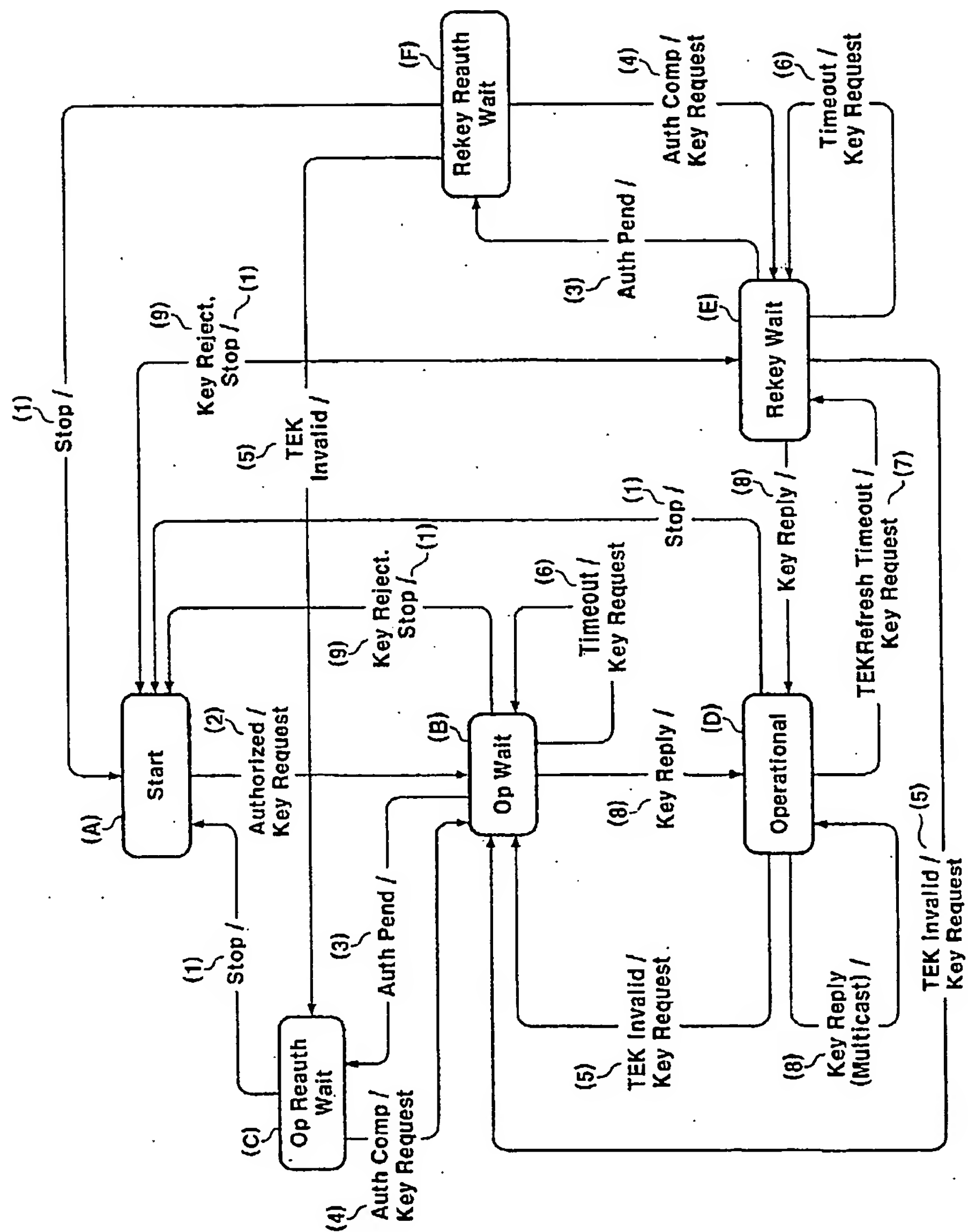
[Fig. 22]

State Event or Rcvd Message	(A) Start	(B) Op Wait	(C) Op Reauth Wait	(D) Op	(E) Rekey Wait	(F) Rekey Reauth Wait
(1) Stop		Start	Start	Start	Start	Start
(2) Authorized	Op Wait					
(3) Auth Pend		Op Reauth Wait			Rekey Reauth Wait	
(4) Auth Comp			Op Wait			Rekey Wait
(5) TEK Invalid				Op Wait	Op Wait	Op Reauth Wait
(6) Timeout		Op Wait		Rekey Wait	Rekey Wait	
(7) TEK Refresh Timeout				Operational	Operational	
(8) Key Reply		Operational				
(9) Key Reject		Start			Start	

FIG. 23

[Fig. 24]

State Event or Rcvd Message	(A) Start	(B) Op Wait	(C) Op Reauth Wait	(D) Op	(E) Rekey Wait	(F) Rekey Reauth Wait	(G) M&B rekey Interim Wait
(1) Stop		Start	Start	Start	Start	Start	
(2) Authorized	Op Wait						
(3) Auth Pend		Op Reauth Wait			Rekey Reauth Wait		
(4) Auth Comp			Op Wait			Rekey Wait	
(5) TEK Invalid				Op Wait	Op Wait	Op Reauth Wait	
(6) Timeout		Op Wait			Rekey Wait		Rekey Wait
(7) TEK Refresh Timeout				Rekey Wait			
(8) Key Reply		Operational			Operational		
(9) Key Reject		Start		Rekey Wait	Start		
(10) GKEK Updated							
(11) TEK Updated							Operational